ГОРИЗОНТ-ВС
ЦИФРОВОЕ БУДУЩЕЕ
НАЧИНАЕТСЯ СЕГОДНЯ

Платформа виртуализации «Горизонт-ВС»

Описание

Оглавление

Платформа виртуализации «Гипервизор-ВС»

Структурная структура комплекса

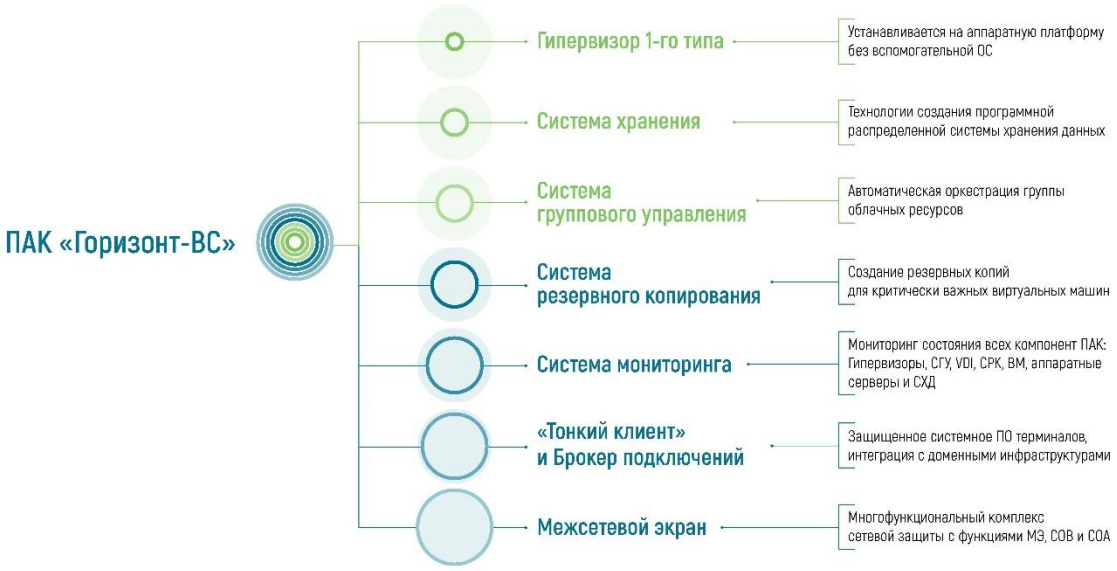

Рисунок 1 - Структурная схема платформы виртуализации верхнего уровня

Схема внедрения платформы

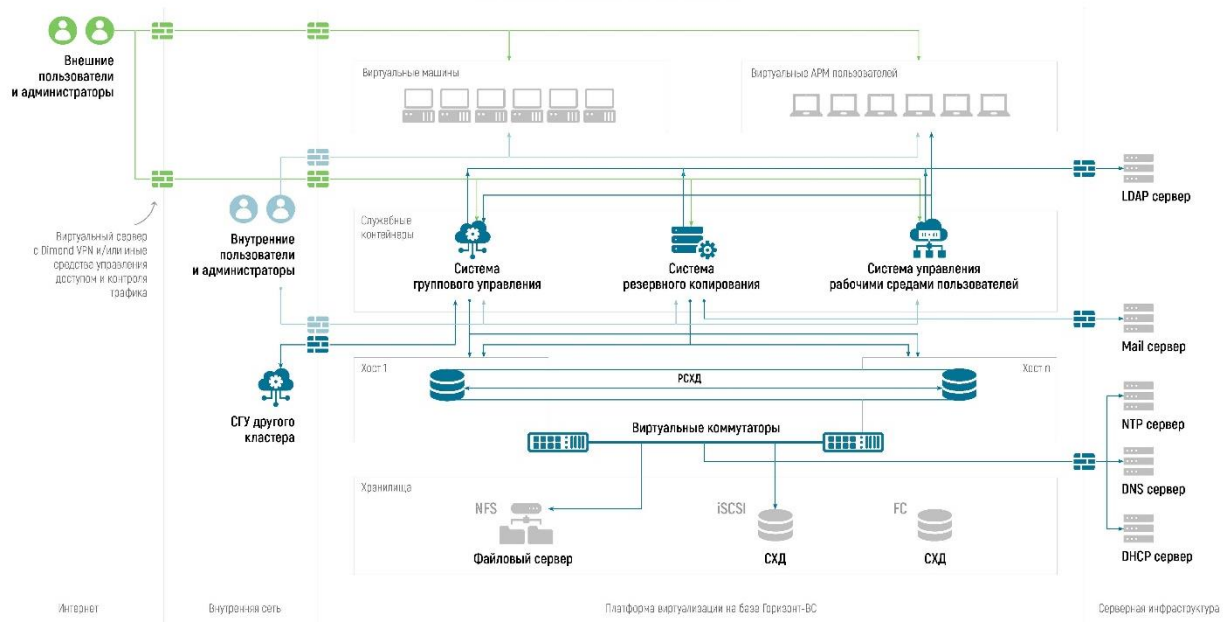

Рисунок 2 – Схема внедрения платформы виртуализации

Описание систем платформы виртуализации «Гипервизор-ВС»

Система виртуализации (Гипервизор)

Функции системы виртуализации

1. Подсистема виртуализации поддерживает возможность загрузки гипервизора с внутреннего или внешнего USB накопителя.
2. Подсистема виртуализации устанавливается непосредственно на аппаратное обеспечение без использования хостовой операционной системы (гипервизор 1 типа).
3. Отсутствует базовая ОС общего назначения в составе гипервизора.
4. Подсистема виртуализации поддерживает технологии оптимизации работы с памятью, такие как Memory Deduplication (KSM), Host Swap, Memory Ballooning, Hugepages.
5. Подсистема виртуализации поддерживает технологию обеспечения отказоустойчивости (кластер высокой доступности (High Availiable)
6. Подсистема виртуализации обеспечивает возможность создания кластера высокой доступности из группы серверов до 200 хостов суммарно.
7. Обеспечена поддержка хост-серверов с количеством логических процессоров до 576 и объемом памяти до 12 ТБ.
8. Подсистема виртуализации обеспечивает возможность миграции функционирующих ВМ между хостами.
9. Подсистема виртуализации обеспечивает возможность миграции функционирующих ВМ между хостами с процессорами разных поколений.
10. Подсистема виртуализации обеспечивает поддержку функции Multipathing.
11. Подсистема виртуализации поддерживает создание программно-определяемой СХД на базе ПО из состава платформы гипервизора.
12. Подсистема виртуализации поддерживает графический установщик.
13. Гипервизор подсистемы виртуализации обеспечивает возможность использования в качестве гостевой операционной системы (ОС) операционных систем семейств Linux, Windows.
14. Подсистема виртуализации поддерживает возможность изменения следующих параметры конфигурации виртуальных машин в процессе функционирования, без приостановки исполнения ВМ:

    — размер дисков;
    — количество дисков;
    — количество сетевых карт.

15. Подсистема виртуализации поддерживает возможность предоставления суммарного объема оперативной памяти виртуальным средам больше, чем доступно на физическом сервере, за счет применения динамического перераспределения памяти между виртуальными средами и освобождением неиспользуемой памяти.
16. Подсистема виртуализации поддерживает возможность автоматического восстановления работы виртуальной среды без человеческого

вмешательства – режим высокой доступности виртуальных машин в случае отказа одного из серверов, дисков или группы физических серверов с помощью автоматического перезапуска виртуальных машин на работоспособных серверах, через переподключение к файлам виртуальных машин, расположенных на общей системе хранения, без потери уже записанных блоков данных на файловую систему.

17. Подсистема виртуализации поддерживает возможность включения или отключения режима высокой доступности для каждой виртуальной машины.
18. Подсистема виртуализации поддерживает поддержку стандарта VirtIO виртуализации дисковых и сетевых устройств.
19. Подсистема виртуализации обеспечивает возможность исполнения виртуальных машин на сервере виртуальных машин изделия в изолированной среде (оперативная и дисковая память виртуальных машин не пересекаются в физическом и виртуальном адресном пространстве).
20. Подсистема виртуализации предоставляет возможность миграции (переноса исполнения) виртуальных машин между серверами виртуальных машин.
21. Подсистема виртуализации обеспечивает создание и хранение образов ВМ для автоматического развертывания ВМ.
22. Подсистема виртуализации обладает встроенными средствами мониторинга.

Система хранения данных

Описание системы хранения данных

Хранилище данных может содержать файлы виртуальных машин (виртуальные диски и описатель виртуальных машин), а также образы ISO.

Система хранения данных поддерживает следующие типы хранилищ:

- хранилище с разделяемым общим диском;
- распределенное хранилище (РСХД) Ceph;
- общая файловая система;
- блочные СХД по протоколам FC/iSCSI/FCoE (lvm.conf);
- файловые СХД по протоколам NFS, CIFS, GFS2, FS;
- проброс блочных устройств хоста.

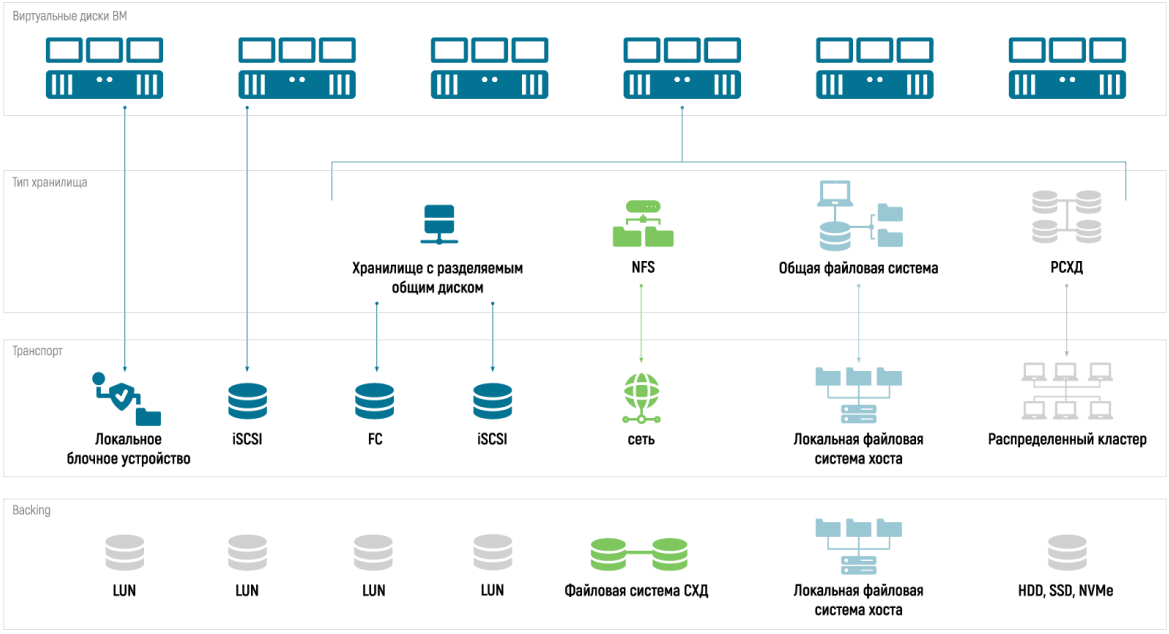

Рисунок 3 - Схема системы хранения данных

В платформе «Горизонт-ВС» реализован отказоустойчивый кластер, основанный на ПО с открытым исходным кодом Pacemaker и Corosync. Он необходим для следующих задач:

1. Для создания кластерного хранилища с числом хостов, равным двум, применяется подход создания реплицируемого блочного устройства DRBD.
2. Для построения кластерного хранилища с числом хостов больше двух применяется подход создания реплицируемого блочного устройства либо распределенной файловой системы средствами сети хранения Ceph.

Функционал системы хранения данных

1. Подсистема хранения данных поддерживает создание программно-определяемой распределённой СХД на базе ПО из состава гипервизора.
2. Подсистема хранения данных обеспечивает хранение данных подсистемы виртуализации.
3. Подсистема хранения данных поддерживает работу в следующих режимах:

   — блочное хранилище данных;
   — файловое хранилище данных;
   — объектное хранилище данных.

4. Подсистема хранения данных обеспечивает отказоустойчивость и сохранность данных при выходе из строя диска, сервера или группы серверов без нарушения работы приложений или прерывания работы пользователей подсистемы хранения.
5. Подсистема хранения данных не имеет единой точки отказа, каждый сервер в кластере данных независимым.
6. Подсистема хранения данных поддерживает создание нескольких кластеров данных на одних и тех же физических серверах.
7. Подсистема хранения данных обеспечивает возможность установки компонентов, отвечающих за работу хранилища на серверах с подсистемой виртуализации, обеспечивая тем самым работу в режиме гиперконвергенции, когда каждый физический сервер используется подсистемой виртуализации и подсистемой хранения данных, являясь частью общего кластера данных.
8. Подсистема хранения данных обеспечивает масштабирование кластера данных с шагом в 1 физический сервер.
9. Подсистема хранения данных обеспечивает возможность объединения локальных дисков, установленных на вычислительных узлах в программно-определяемое распределенное дисковое хранилище.
10. Подсистема хранения данных обеспечивает возможность использования подключенных к физическим серверам дисковых полок класса JBD.
11. Подсистема хранения данных обеспечивает возможность подключения к хранилищу данных с помощью клиента, установленного на подсистеме виртуализации без использования Fibre Channel, iSCSI.
12. Подсистема хранения данных обеспечивает возможность одновременного использования дисков SSD, SAS и SATA разной емкости для реализации хранилища данных.
13. Подсистема хранения данных обеспечивает возможность фиксации за виртуальной машиной использования определенного уровня хранилища данных (по скорости записи).
14. Подсистема хранения данных обеспечивает возможность предоставления доступа к хранилищу данных через протоколы iSCSI, Fibre Channel, NFS, CIFS/SMB.
15. Подсистема хранения данных обеспечивает возможность синхронной репликации каждого блока записанных данных и возвращать подтверждение выполнения операции записи блока данных приложениям после записи всех реплик.
16. Подсистема хранения данных обеспечивает возможность создания реплик в количестве не менее 3.

17. Подсистема хранения данных обеспечивает возможность использования ультрабыстрых SSD дисков под хранение журналов для увеличения производительности на запись хранилища.
18. Подсистема хранения данных обеспечивает возможность использования ультрабыстрых SSD дисков для хранения кэша для увеличения производительности на чтение хранилища.
19. Подсистема хранения данных обеспечивает возможность добавления новых дисков и серверов в кластер без прерывания работы.
20. Подсистема хранения данных поддерживает клиентскую часть, которая позволяет получать доступ ко всему объёму хранилища данных с систем, на которые она установлена.
21. Подсистема хранения данных поддерживает назначение ролей для серверов:

    — сервер хранения (только хранение данных);
    — сервер метаданных (управление картой данных).

22. Подсистема поддерживает подключение разделяемых СХД по протоколам NFS, iSCSI и Fibre Channel.
23. Подсистема обеспечивает создание конвергентных и гиперконвергентных решений на базе платформы.
24. Подсистема обеспечивает поддержку функции Multipathing.

Система распределенных виртуальных коммутаторов

Описание системы распределенных виртуальных коммутаторов

В Платформе серверной виртуализации «Гипервизор-ВС» по умолчанию применяются распределенные виртуальные коммутаторы. За счет распределенной базы конфигураций все создаваемые виртуальные коммутаторы становятся распределенными. Каждый распределенный виртуальный коммутатор позволяет работать с любым количеством VLAN, вплоть до 4096 штук.

Виртуальный коммутатор хоста обеспечивает:

- подключение виртуальных машин к физической сети ЦОД;
- взаимосвязь между виртуальными машинами на одном и том же хосте (в пределах виртуальной сети);
- передачу служебного трафика (управление хостом, трафик iSCSI, NFS).

Функции системы распределенных виртуальных коммутаторов

1. Сетевая система обеспечивает поддержку виртуальных коммутаторов.
2. Сетевая система поддерживает работу в режимах:

   - Open vSwitch (+Ip route);
   - Bridged;
   - Bridged & Security Groups;
   - Bridged with ebtables VLAN;
   - 802.1QVLAN (стандартный VLAN);
   - VXLAN

3. Сетевая система поддерживает использование для изоляции и/или объединения в виртуальные сети сетевого трафика виртуальных машин протоколы VLAN, VXLAN.

Система группового управления

Описание системы группового управления

Система группового управления платформой «Горизонт-ВС» – высокоуровневое средство управления облачной инфраструктурой через веб-интерфейс, которое состоит из следующих подсистем:

- управления пользователями и группами;
- управления виртуализацией;
- управления хостами;
- мониторинга показателей доступности, производительности и степени загруженности, контролируемых виртуальных и физических ресурсов;
- сбора статистики;
- управления виртуальными сетями;
- управления хранилищами;
- обеспечения высокой доступности;
- кластерной подсистемы;
- создания и управления зонами;
- организации виртуального изолированного облака.

Функционал системы группового управления

1. Система управления подсистемой виртуализации использует веб-интерфейс.
2. Система управления подсистемой виртуализации имеет возможность обеспечения доступа к локальным консолям виртуальных машин через веб-интерфейс управления средствами протоколов VNC или SPICE.
3. Система управления подсистемой виртуализации обеспечивает вывод в интерфейс управления информации о виртуальных машинах, пулах ресурсов, узлах.
4. Система управления подсистемой виртуализации обеспечивает возможность управления виртуальными средами посредством графического интерфейса в следующем объёме:

   - создание и редактирование виртуального окружения виртуальных машин (формирование виртуальной аппаратной конфигурации: определение количества процессоров, объёма оперативной памяти, количества и объёма дисков, количества и параметров сетевых интерфейсов);
   - регистрация физических серверов виртуализации;
   - создание логических структур (кластеров) на базе физических серверов виртуализации;
   - создание и управление шаблонами виртуальных машин;
   - создание и управление образами виртуальных машин;
   - управление ресурсами виртуальных машин (ЦПУ, оперативная память, дисковое пространство);
   - управление и добавление устройств в виртуальные машины;
   - управление и добавление устройств в виртуальные машины;
   - добавление дисков в виртуальные машины в процессе исполнения, без остановки исполнения виртуальных машин;

- добавление виртуальных сетевых интерфейсов в ВМ, без остановки исполнения виртуальных машин;
- изменение размеров виртуальных дисков ВМ из графического интерфейса, без остановки исполнения виртуальных машин;
- выполнение групповых операций с виртуальными машинами;
- мониторинг загрузки процессора, памяти, диска и сети в виртуальных машинах;
- управление Системами формирования отказоустойчивого кластера;
- создание и редактирование виртуальных сетевых мостов;
- возможность миграции виртуальных дисков в процессе работы виртуальных машин;
- возможность миграции функционирующих виртуальных машин между хостами с процессорами разных поколений.

Система резервного копирования

Описание системы резервного копирования

Подсистема резервного копирования обеспечивает возможность выполнения резервного копирования виртуальных сред средствами подсистемы виртуализации в запущенном и остановленном состоянии (полное и инкрементальное) по заданному расписанию с возможностью последующего управления резервными копиями.

Подсистема резервного копирования поддерживает возможность восстановления резервных копий средствами подсистемы виртуализации на любом из серверов. Подсистема резервного копирования поддерживает возможность удаления инкрементальных резервных копий из цепочки без потери разрыва цепочки резервных копий.

Система резервного копирования предназначена для выполнения операций по защите данных в виртуальной среде путем резервного копирования с целью последующего восстановлению данных в случае аварийных ситуаций. Модуль интегрирован с Системой Группового Управления (СГУ) платформы виртуализации «Горизонт-ВС». Разграничение прав пользователей на запуск модуля осуществляется средствами СГУ.

Система состоит из 3-х основных компонент:

- web-интерфейс управления;
- компонент обработки заданий;
- исполнительный компонент («агент»).

Все три компонента работают асинхронно.

Функционал системы резервного копирования

1. Подсистема резервного копирования обеспечивает возможность выполнения резервного копирования виртуальных сред средствами подсистемы виртуализации в запущенном и остановленном состоянии (полное и инкрементальное) по заданному расписанию с возможностью последующего управления резервными копиями.
2. Подсистема резервного копирования поддерживает возможность восстановления резервных копий средствами подсистемы виртуализации на любом из серверов.
3. Подсистема резервного копирования поддерживает возможность удаления инкрементальных резервных копий из цепочки без потери разрыва цепочки резервных копий.

Система «Брокер» VDI

Описание системы «Брокер» VDI

Инфраструктура виртуальных рабочих столов (VDI) – это программный инструмент для централизованного создания виртуальных рабочих столов и управления ими.

Брокер подключений VDI– это программное обеспечение, которое облегчает удаленное соединение между конечными пользователями и сервером, установленным на гипервизоре. Когда пользователь подключается к сервисам удаленных рабочих столов, этот программный уровень аутентифицирует пользователя и предоставляет ему доступ к среде виртуального рабочего стола. Это также облегчает взаимодействие между удаленным пользователем и виртуальным рабочим столом.

Функциональные особенности VDI

1. Подсистема VDI включает ПО тонкого клиента с возможностью выбора рабочего стола для подключения из списка, предоставляемого пользователю после авторизации.
2. Подсистема VDI обеспечивает подключение USB устройств пользователя через терминал тонкого клиента к виртуальному рабочему месту.
3. Подсистема VDI обеспечивает воспроизведение FullHD видео на виртуальном рабочем месте пользователя.
4. Подсистема VDI обеспечивает управление публикацией рабочих столов и приложений на основании членства пользователей в группах безопасности Active Directory/Open LDAP.
5. Подсистема VDI обеспечивает ограничение выделения ресурсов под нужды конкретного пользователя.
6. Подсистема VDI обеспечивает печать на локальные и сетевые принтеры, подключенные на рабочем месте пользователя.
7. Обеспечена установка безопасного соединения между тонким клиентом и гипервизором.

Система информационной безопасности

Описание Системы информации безопасности

Система виртуализации является сертифицированным по требованиям ФСТЭК средством защиты информации, и обладает функционалом, предназначенным для защиты критической информационной инфраструктуры (КИИ). Сертификат ФСТЭК России УД-4, СВТ-5, ИТ.СДЗ.ПР4.ПЗ, обеспечивает защиту ГИС класса К1 и ИСПДн класса защищённости К-1.

Функционал Системы информационной безопасности

1. Подсистема виртуализации предоставляет возможность исполнения виртуальных машин на аппаратном обеспечении в гарантированно изолированной среде (оперативная и дисковая память виртуальных машин не пересекаются в физическом и виртуальном адресном пространстве).
2. Подсистема виртуализации обеспечивает возможность контроля целостности ядра системы средствами модуля доверенной загрузки.
3. В составе гипервизора отсутствуют базовые ОС общего назначения.
4. Подсистема виртуализации обеспечивает возможность функционирования виртуальных систем обнаружения вторжения, межсетевых экранов, антивирусных средств, средств анализа защищенности, средств защиты информации от DDoS атак, средств корреляции событий безопасности, средств контроля утечки информации из информационной системы.

Система мониторинга

Описание системы мониторинга

В Платформе виртуализации «Гипервизор-ВС» используется глобальная система мониторинга всех компонентов кластера: узлы, сети, виртуальные машины, внешние СХД и прочее. Система мониторинга позволяет обрабатывать и хранить большие объемы статистической информации, на основе которой администраторы Платформы могут легко получать необходимую информацию.

Функционал системы мониторинга

1. Возможность отслеживание следующих показателей состояния Гипервизоров:

   — загрузка процессора;
   — загрузка оперативной памяти;
   — загрузка логических разделов дисковой подсистемы;
   — доля потерянных сетевых пакетов;
   — средний RTT;
   — количество размещенных виртуальных машин.

2. Возможность отслеживание следующих показателей состояния Системы Группового Управления:

   — состояние работы веб-сервера;
   — состояние работы СУБД;
   — состояние работы служб ППО СГУ;
   — состояние контейнера.

3. Возможность отслеживание следующих показателей состояния подсистемы резервного копирования:

   — состояние работы веб-сервера;
   — состояние работы ППО подсистемы СРК;
   — состояние контейнера.

4. Возможность отслеживание следующих показателей состояния подсистемы VDI:

   — состояние работы ППО подсистемы VDI;
   — состояние контейнера.

5. Возможность отслеживание следующих показателей состояния кластеров хранилищ данных распределённой СХД:

   — загрузка дисковой подсистемы кластера хранилища данных;
   — состояние работы кластера.

6. Возможность отслеживание следующих показателей состояния системы виртуальной коммутации:

- состояние служб виртуальной коммутации;

7. Возможность отслеживание следующих показателей виртуальных машин агентским способом:

   - загрузка процессора;
   - загрузка оперативной памяти;
   - загрузка логических разделов дисковой подсистемы;
   - загрузка сетевых интерфейсов.

8. Возможность отслеживание следующих показателей физического оборудования, задействованного в работе виртуализации по технологии Redfish:

   - состояние дисков;
   - состояние процессоров;
   - состояние модулей оперативной памяти;
   - состояние системы охлаждения;
   - состояние блоков питания;
   - состояние сетевых карт.

9. Возможность настройки уведомлений по электронной почте и смс о зафиксированных отклонениях отслеживаемых показателей от нормальных значений.
10. Возможность формирования отчетов за определенный временной период о фактах выявленных отклонений и нарушений пороговых значений за период.

Система «Межсетевой экран»

Описание системы МКСЗ «Горизонт-ВС»

Система «Межсетевой экран» (МКСЗ «Горизонт-ВС»)» является решением, которое включает в себя основные функции: защита каналов передачи данных, межсетевое экранирование, обнаружение и отражение атак.

Все функции как основные, так и дополнительные (динамическая маршрутизация, механизмы отказоустойчивости и резервирования, возможность работать в режиме коммутатора и др.) могут работать одновременно на одном устройстве. Гибкая модульная архитектура позволяет эффективно реализовывать любые политики безопасности и с наименьшими затратами осуществлять интеграцию решения в текущую сетевую инфраструктуру.

МКСЗ «Горизонт-ВС» имеет интуитивно понятный графический интерфейс для настройки и управления функциями безопасности и легко интегрируется в любую информационную инфраструктуру. Устройства МКСЗ «Горизонт-ВС» могут быть объединены в единую группу подчиненных устройств под управлением центра управления и мониторинга, что позволяет настраивать, управлять и осуществлять мониторинг подчиненных программно-аппаратных комплексов с единой консоли управления.

Функционал системы МКСЗ «Горизонт-ВС»

1. Ключевые функциональные возможности

   - высокоскоростное шифрование в каналах связи;
   - поддержка L2overVPN, L3overVPN;
   - межсетевой экран в режиме работы L2/L3;
   - система обнаружения и предотвращения;
   - вторжений (кроме 0-й и 1-й серии).

2. Ключевые преимущества

   - высокая скорость шифрования
   - низкая вносимая задержка до 2 мс
   - высокая надежность компонентов и их резервирование
   - размещение в стойке (кроме 0-й и 1-й серии)
   - максимальная плотность портов (6-я и 7-я серии)
   - четыре дополнительных модуля расширения (6-я и 7-я серии)
   - высокая доступность и масштабируемость